METHOD AND APPARATUS FOR ASSIGNING CONDITIONAL OR CONSEQUENTIAL RIGHTS TO DOCUMENTS AND DOCUMENTS HAVING SUCH RIGHTS

Related Application Data

mc 1/20/04

[0001] This application is related to Applicants' patent applications entitled METHOD AND APPARATUS FOR TRANSFERRING USAGE RIGHTS AND DIGITAL WORK HAVING TRANSFERRABLE USAGE RIGHTS (~~Attorney Docket No. 111325-63~~ U.S. Application No. 09/867,746), METHOD AND APPARATUS FOR ESTABLISHING USAGE RIGHTS FOR DIGITAL CONTENT TO BE CREATED IN THE FUTURE (~~Attorney Docket No. 111325-68~~ U.S. Application No. 09/867,747), DEMARCATED DIGITAL CONTENT AND METHOD FOR CREATING AND PROCESSING DEMARCATED DIGITAL WORKS (~~Attorney Docket No. 111325-62~~ U.S. Application No. 09/867,754), METHOD AND APPARATUS FOR DYNAMICALLY ASSIGNING USAGE RIGHTS TO DIGITAL WORKS (~~Attorney Docket No. 111325-66~~ U.S. Application No. 09/867,745), and METHOD AND APPARATUS FOR HIERARCHICAL ASSIGNMENT OF RIGHTS TO DOCUMENTS AND DOCUMENTS HAVING SUCH RIGHTS (~~Attorney Docket No. 111325-65~~ U.S. Application No. 09/867,748), which are being filed concurrently herewith, and are incorporated herein by reference in their entirety.

Background of the Invention

Field of the Invention

[0002] This invention relates to the assignment of rights to a document. In particular, this invention relates to the assignment of conditional or consequential rights to one or more documents, and the management of those documents.

Description of Related Art

[0003] Digital rights management (DRM) describes a process of attaching usage rights to a digital work, such as eContent, as well as managing and enforcing the same rights. In general, these digital works and eContent can include any type of content, such as music, books, multimedia presentations, eBooks, video information, or the like. In general, any information that is capable of being stored can be protected through the use of digital rights management. For example, a digital book could be accompanied by a license establishing conditions, such as viewing, printing, borrowing, or the like, governing the book's usage. These rights could then be controlled by, for example, an associated reader's software, and the allowable transactions, such as buying, printing, or the like, authorized by, for example, a clearinghouse.

[0004] One of the most important issues impeding the widespread distribution of digital works as documents via electronic means, such as the internet, is the lack of protection of intellectual property rights of content owners during the distribution, dissemination and use of those digital documents. Efforts to overcome this problem have been termed "intellectual property rights management" (IPRM), "digital property rights management" (DPRM), "intellectual property management" (IPM), "rights management" (RM) and "electronic copyright management" (ECM), which can be collectively referred to as Digital Rights Management (DRM). There are a number of issues in Digital Rights Management including authentication, authorization, accounting, payment and financial clearing, rights specifications, rights verification, rights enforcement, document protection, and the like.

[0005] In the world of printed documents, a work created by an author is typically provided to a publisher, which formats and prints numerous copies of the work. The copies are then distributed to bookstores or other retail outlets, from which the copies are purchased by end users. While the low quality of physical copying, and the high cost of distributing printed material have served as deterrents to unauthorized copying of most printed documents, digital documents allow easy copying, modification, and redistribution if they are unprotected. Accordingly, digital rights management allows the protecting of digital documents to, for example, complicate copying, modifying and redistributing.

[0006] Similarly, it has been widely recognized that it is difficult to prevent, or even deter, individuals from making unauthorized distributions of electronic documents within current general-purpose computer and communication systems such as personal computers, workstations, and other devices connected via a distributed network, such as a local area network, an intranet and the internet. Many attempts to provide hardware-based solutions to prevent unauthorized copying have proven to be unsuccessful. Furthermore, the proliferation of broadband communications technologies and the development of the "national information infrastructure" (NII) will likely make it even more convenient to distribute large documents electronically, thus removing most deterrents to any unauthorized distribution of documents. Therefore, digital rights management technologies provide one method of protecting digital documents distributed electronically.

[0007] Two basic schemes have been employed to attempt to solve the document protection problem. In particular, the two basic schemes are secure containers and trusted systems. A secure container, or simply an encrypted document, offers one method of keeping document contents encrypted until a set of authorization parameters are satisfied. After the various parameters are verified, for example, by the document provider, the document can be released to a user. Commercial products such as IBM's Cryptolopes® and InterTrusts Digiboxes® fall into this category. While the secure container approach provides a solution to protect the document during delivery over unsecure channels, it does not provide any mechanism to prevent legitimate users from obtaining the unencrypted document, and then, for example, using and redistributing the unprotected document without authorization.

[0008] In the trusted system approach, the entire system that handles, for example, the distribution and viewing of a document, is responsible for preventing unauthorized use. Building such a trusted system usually entails introducing new hardware such as a secure processor, a secure storage, and secure rendering devices. The trusted system also requires that all software applications that run on the system be certificate to be trusted.

[0009] U.S. Patent Nos. 5,530,235, 5,634,012, 5,715,403, 5,638,443 and 5,629,980, which are incorporated herein by reference in their entirety, generally discuss digital rights

management. In general, an author creates a document and forwards it to a distributor for distribution. Typically, the author is the creator of the content, however, the author can be any one of the creator, the owner, the editor, or any other entity controlling a portion of content, or an agent of one of those entities. The author may distribute documents directly, without involving a secondary party such as a distributor. Therefore, the author and the distributor may be the same entity. A distributor can distribute documents to one or more users, for example, upon request. In a typical electronic distribution model, the content can be distributed as a document in encrypted form. For example, a distributor can encrypt the content with a random key, having encrypted the random key with a public key corresponding to one or more users. Thus, the encrypted document can be customized solely for a particular user. The user is then able to use the private key to unencrypt the public key and use the public key to unencrypt and view the document.

[0010] Payment for the document can be passed from a user to a distributor by way of a clearinghouse which can collect requests from one or more users who wish to view a particular document. The clearinghouse can also collect payment information, such as debit transactions, credit transactions, credit card transactions, or other known electronic payment schemes and forward the collected payments to a distributor. Furthermore, the clearinghouse may retain a share of the payment as a fee for these services. The distributor may also retain a portion of the payment from the clearinghouse to cover, for example, distribution services and royalties due an author.

[0011] Each time the user requests a document, an accounting message can be sent to an accounting server that can, for example, ensure that each request by the user matches a document sent by the distributor. Additionally, the accounting information can be received by an accounting server and distributor to reconcile any inconsistencies.

SUMMARY OF THE INVENTION

[0012] Conditional or consequential rights associated with a document allow for the limited usage of content based on, for example, an absolute value, a relative value, or the like. For example, the starting period of a right based on another event or another right can

trigger the availability or expiration of availability of a document. Furthermore, the time for limiting the usage of content can be expressed as an absolute value, such as a particular time and date, or a relative value, such as a usage right expiring two minutes after a first usage. The usage right can also be linked to other events, such as the expiration of a right of another document, or the like. For example, a piece of music could be listened to for only one minute, or it can be listened to only once, after the right to a second piece of music has expired. This conditional or consequential right assignment can be hierarchical, such as the systems and methods described in co-pending ~~Attorney Docket No. 111325.65,~~ U.S. Application No. 09/867,748 entitled "Method and Apparatus for Hierarchical Assignment of Rights to Documents and Documents Having Such Rights," filed herewith and incorporated by reference in its entirety, and/or linked to other events that may or may not have more than one step or condition. For example, the condition could be a chain of events that trigger the conditional or consequential rights. An example of this can be used in remote learning schemes. For example, if college courses are offered on the internet, the courses can be offered at a specified time, or the access to a second course restricted until a first course has been viewed.

1/20/04 mc

[0013] In another example, if an exam has five sections, and for each section, a thirty-minute period is allocated, the user can proceed to the next section by using the thirty allocated minutes, or by pushing a button on, for example, a user interface, which indicates that they have completed that section. Alternatively, other triggering events and/or conditions can also govern transition to a subsequent document based on, for example, a fifteen-minute break allocated between sections 3 and 4. In this exemplary embodiment, multiple timers or counters can keep track of the time for each section and/or for all of the sections combined.

[0014] Alternative, the test taker could switch back and fourth between different sections, as long as the time is within the allocated time for each section or within other thresholds, such as a fifty-minute maximum for any given section. Alternatively, in another exemplary embodiment, alternating between sections may be forbidden. In this exemplary embodiment, time allocations can be based on multiple rules, and counters may or may not

be dependent on each other, as a test administrator sets the rules and constraints of the exam prior to administration of the exam.

[0015] This concept can include the concept of subsidiary rights, for which one grants a right to a user, provided the user satisfies some condition or performs an action. For example, a user can edit one a copy is made of a document.

[0016] As another example, for joint projects, more than one person may contribute to the document with comments and modifications and/or design changes in which case a digital rights management system can keep track of, exercised rights, modifications, sources of modifications, dates, order of changes, approvals, vetoes, priorities, or the like. For example, in a paperless office, three approvals from three different departments may be needed for an action item.

[0017] The right assignment can also be integrated into, for example, an e-mail or electronic messaging system. For example, a content owner can assign different rights to different individuals and share or limit rights to information or files based on those rights. A friend could request permission to view or use a particular file, or further distribute the file to another individual, everyone in the address book or the public as a whole. Alternatively, the rights could, for example, limit the extent to which a user can add or delete individuals from a mailing list or address book. The right to view people in an address book could also be restricted based on a usage right. As another example, while in an instant messaging mode, a user can have the right to exclude or limit other users to particular content.

[0018] If the set of assigned rights are commonly used for different documents, the rules can be expressed as, for example, templates such as those discussed in U.S. Provisional Application Serial No. 60/261,753, entitled "Method and Apparatus for Editing and Specifying the Rights and Conditions Associated with Documents or digital contents, incorporated herein by reference in its entirety, multi-hyphen purpose templates, or the like. In general, a template can be used whenever a user desires to assign a predetermined set of rights to one or more, such as a set, of additional users. This template can contain, for

example, a set of usage rights that may be particularly tailored towards the user class, accounting instructions, or the like.

[0019] In another exemplary embodiment, assume a content owner desires to assign some rights to a user, in terms of what compression methods the user can employ on the original data. For example, for some data, the content owner may wish to let the user be able to compress the data only by one of the choices of lossless compression techniques to maintain the integrity of the data. Alternatively, in another situation, for specific data the content owner may desire to let the user compress the data only by one of the choices of lossy methods, as long as the bit rate or total size of the document stays below a threshold.

[0020] For multilevel databases, some parts of the data may be open to public, while other parts may require different levels of rights or security clearance, such as differentiated security, using attribute-level sensitivity. For example, in a company, the telephone number of the employees may be accessible to the other employees, while other personal information, such as personnel information, cannot be accessed unless the content user is within a predefined class. For example, the direct supervisor may have access to inspect, read or modify the employee's personnel file, as long as a "paper trail" which records information pertaining to the supervisor's changes is generated and associated with the file. Furthermore, the right to notarize particular content, such as the electronic-signature of an authorized entity and/or a time stamp, with the option of an encryption for safe storage, can also be granted separately by a content owner.

[0021] Aspects of the present invention relate to assigning rights to documents. In particular, rights based on conditional or consequential conditions can be associated with a document.

[0022] Additionally, aspects of the present invention relate to a system for assigning conditional or consequential rights to one or more documents.

[0023] Furthermore, aspects of the present invention relate to activating or restricting access to one or more documents based on a conditional or consequential right associated with that document.

[0024] These and other features and advantages of this invention are described in, or are apparent, from the following detailed description of the embodiments.

BRIEF DESCRIPTION OF THE DRAWINGS

[0025] The embodiments of the invention will be described in detail, with reference to the following figures wherein:

[0026] Fig. 1 is a functional block diagram illustrating an exemplary document according to this invention;

[0027] Fig. 2 illustrates an exemplary conditional or consequential right assignment according to this invention;

[0028] Fig. 3 illustrates an exemplary conditional or consequential right assignment according to this invention;

[0029] Fig. 4 illustrates an exemplary conditional or consequential right assignment according to this invention;

[0030] Fig. 5 illustrates an exemplary conditional or consequential right assignment according to this invention ~~ntion;~~

[0031] Fig. 6 illustrates an exemplary conditional or consequential right assignment according to this invention;

[0032] Fig. 7 illustrates an exemplary conditional or consequential right assignment according to this invention;

[0033] Fig. 8 illustrates an exemplary conditional or consequential right assignment according to this invention;

[0034] Fig. 9 is a flowchart outlining an exemplary method for assigning rights according to this invention; and

[0035] Fig. 10 is a flowchart outlining an exemplary method for exercising a right based on a condition or consequence according to this invention.

DETAILED DESCRIPTION OF THE INVENTION

[0036] Typically, rights are assigned to one or more documents based on, for example, a license agreement with the content owner. These rights are generally static and can be exercised by a user at any time provided the conditions of the license agreement, such as payment, are satisfied. By modifying the management of these rights, an exemplary embodiment of the systems and methods of this invention allow for specific portions of the rights associated with a specific portion of a document to be triggered based on, for example, a conditional or consequential event.

[0037] For example, a document can have one or more rights associated with it which may include one or more usage rights and/or delegation rights. The usage rights specify, for example, the right a particular user has to the document such as viewing, editing, modifying, updating, printing, or the like. The delegation rights include, for example, to how many users a user can distribute the document to, and which rights the user is allowed to associate with those distributed documents.

[0038] Thus, by associating a conditional or consequential trigger with the one or more usage rights and delegation rights, a content owner can provide additional specificity governing the use of one or more documents.

[0039] Fig. 1 illustrates an exemplary document 100. The document 100 comprises a right management module 110, a right availability module 120, a tracking module 130, a right usage determination module 140, an interface module 150, an accounting module 160, and a document updating module 170, interconnected by link 5. The document 100 can also

be connected to a distributed network (not shown) which may or may not also be connected to one or more other documents, account processing systems, rights management systems, or other distributed networks, as well as one or more input devices and display devices (not shown).

[0040] While the exemplary embodiment illustrated in Fig. 1 shows the document 100 and associated components collocated, it is to be appreciated that the various components of the document 100 can be located at distant portions of a distributed network, such as a local area network, a wide area network, an intranet and/or the Internet, or within a dedicated document or document system. Thus, it should be appreciated that the components of the document 100 can be combined into one device or collocated on a particular note of distributed network. Furthermore, it should be appreciated that for ease of illustration, the various functional components of the document 100 have been divided as illustrated in Fig. 1. However, any of the functional components illustrated in Fig. 1 can be combined or further partitioned without affecting the operation of the system. As will be appreciated from the following description, and for reasons of computation efficiency, the components of the document can be arranged at any location within a distributed network without effecting the operation of the system. Furthermore, it is to be appreciated that the term module as used herein includes any hardware and/or software that provide the functionality as discussed herein. Likewise, the document 100 can comprise any necessary controllers, memory, and/or I/O interfaces that may be necessary given the particular embodiment and/or implementation of the document 100. Additionally, the document 100 can be any information to which conditional and/or consequential rights are associated.

[0041] Furthermore, the links 5 can be a wired or wireless link or any other known or later developed element(s) that is capable of supplying and communicating data to and from the connected elements. Additionally, the input devices can include, for example, a keyboard, a mouse, a speech to text converter, a stylus, a mouse, or the like. In general, the input device can be any device capable of communicating information to the document 100. Furthermore, the display device can be a computer monitor, a display on a PDA, an E-Book, or any other device capable of displaying information to one or more users.

[0042] Upon receiving a request by a user to use a document, the right availability module 120, in cooperation with the right management module110 and the interface module 150 monitors the condition or consequential triggers associated with the document. Upon satisfaction of one or more of the conditional or consequential event, the document is released to the user for the requested use and any necessary accounting, such as crediting and/or debiting performed. Then, if the conditional or consequential right has an associated termination or expiration portion, the right availability module 120 in cooperation with the right management module 110 and the interface module 150 terminate the user's usage and/or delegation rights.

[0043] Fig. 2 illustrates an exemplary document 200 comprising one or more usage rights 210 and or one more delegation rights 220. Each of the usage rights 210 and the delegation rights 220 can also have associated therewith conditional/consequential rights 230 and 240, respectively. As previously discussed, this allows the usage rights to be based on, for example, the completion of a particular event or condition. Similarly, the delegation rights can be restricted based on a particular condition or event.

[0044] Figs. 3-8 illustrate exemplary conditional events and subsequent rights granted to users. In particular, Fig. 3 illustrates that after condition A commences, a user has a view right for a predetermined duration.

[0045] In Fig. 4, after a condition B starts, a first user has a view right associated with a document. Additionally, a second user has a view right that it limited to a predetermined duration.

[0046] In Fig. 5, if an exemplary user in possession of the document is known, via, for example, a smart card, an identification, such as driver's license, a fingerprint, or the like, and the user's identity matches the conditional right, the user has view and edit rights for the document.

[0047] In Fig. 6, if an exemplary predetermined condition occurs, a first user has distribution rights, and a second user has an approval right for a predetermined duration. For example, the conditional event could be a stock offering that the first user can distribute.

The second user can then be granted the option to purchase stock at, for example, a preferred price, for 24 hours. After 24 hours, this right to purchase can be withdrawn, and the second user's access to the document restricted.

[0048] Fig. 7 illustrates an exemplary conditional event where a predetermined time after a first condition ends or a second condition starts, subsequent rights are available. In this exemplary embodiment, after the triggering event, a first user has view and modify rights, while a second user is granted one print right.

[0049] In Fig. 8, the triggering event is when a predetermined condition ends. Upon satisfaction of this triggering event, rights are removed from the document possessed by the user. For example, the document can monitor the current date and time and once that time has passed, restrict access to the document.

[0050] Fig. 9 illustrates an exemplary embodiment of a method for associating conditional and/or consequential rights with a document. In particular, control begins in step S100 and continues to step S110. In step S110, a determination is made whether rights are already associated with the document. If rights are associated with the document, control continues to step S120 where the usage and delegation rights available to the particular user are determined. Control then continues to step S130.

[0051] In step S130, the rights one or more users desire to have associated with the document are received. Next, in step S140, it is determined whether the assignment of these rights is allowable. If the assignment is allowable, control continues to step S160. Otherwise, control jumps to step S150. In step S150, a message can be forwarded to the user indicating the assignment is not available. Control then optionally continues back to step S130.

[0052] In step S160, an optional accounting function can be performed. If accounting is necessary, control continues to step S170. Otherwise, control jumps to step S200.

[0053] In step S170, any necessary accounting functions are attempted. Then, in step S180, a determination is made whether the accounting, e.g., any crediting and/or debiting, is

allowed. If the accounting functions are successful, control jumps to step S200. Otherwise, control continues to step S190 where a message can be forwarded to the user and control returns back to step S130.

[0054] In step S200, the right as chosen by the one or more users are associated with the document. Then, in step S210, the document can be updated reflecting, for example, which usage rights were used, the effect of any of these usage rights, a signature of the user and, for example, any modifications to or assignment of delegation rights. Control then continues to step S200 where the control sequence ends.

[0055] Fig. 10 illustrates an exemplary method of activating a right based, which could grant or restrict access, based on one or more conditions. In particular, control begins in step S400 and continues to step S410. In step S410, one or more conditions are monitored for detection of a triggering event. Then, in step S420, a determination is made whether the triggering event has been satisfied. If the triggering event is present, control jumps to step S450, otherwise, control continues to step S430. In step S430, a determination is made whether the conditional triggering event has expired. If the triggering event has expired, control jumps to step S510 where the control sequence ends. Otherwise, control continues to step S440, where the system waits for the triggering event and returns to step S410.

[0056] In step S450, a determination is made whether any accounting actions are necessary. If accounting actions are required, control continues to steps S460. Otherwise, control jumps to step S490.

[0057] In step S460, any necessary accounting, such as debiting and/or crediting is performed. Next, in step S470, a determination is made whether the debiting and/or crediting was successful. If the accounting was successful, control jumps to step S490, otherwise, control continues to step S480, where a message can be forwarded to the user indicating a problem associated with the accounting. Control then continues to step S510.

[0058] In step S490, one or more users are granted access to one or more documents based on the associated usage and delegation rights. Next, in step S500, the usage rights can be updated, for example, by associating a digital signature with the document that

corresponds to, for example, the identify of the user and/or any modifications the user may have made to the document and any delegations performed by that user. Control then continues to step S510 where the control sequence ends.

[0059] As illustrated in Fig. 1, the document can be implemented either on a single programmed general purpose computer or a separate programmed general purpose computer. However, the document can also be implemented on a special purpose computer, a programmed microprocessor or microcontroller and peripheral integrated circuit element, an ASIC or other integrated circuit, a digital signal processor, a hardwired electronic or logic circuit such as a discrete element circuit, a programmable logic device such as a PLD, PLA, FPGA, PAL, or the like. In general, any device capable of implementing a finite state machine that is in turn capable of implementing the flowcharts in Figs. 9-10 can be used to implement the document and conditional/consequential rights management system according to this invention.

[0060] Furthermore, the disclosed method may be readily implemented in software using object or object-oriented software development environments that provide portable source code that can be used on a variety of computer or workstation hardware platforms. Alternatively, the disclosed document and right management system may be implemented partially or fully in hardware using standard logic circuits or VLSI design. Whether hardware or software is used to implement the systems and methods in accordance with this invention is dependent on the speed and/or efficiency requirements of the system, the particular function, and a particular software and/or hardware systems or microprocessor or microcomputer systems being utilized. The document and rights management systems illustrated herein, however, can be readily implemented in hardware and/or software using any known or later-developed systems or structures, devices and/or software by those of ordinary skill in the applicable art from the functional description provided herein and with a general basic knowledge of the computer arts.

[0061] Moreover, the disclosed methods may be readily implemented as software executed on a programmed general purpose computer, a special purpose computer, a microprocessor or the like. In these instances, the methods and systems of this invention

can be implemented as a program embedded in a personal computer, an E-Book, a secure container, or the like, such as a Java® or CGI script, as an XML document, as a resource residing on a server or graphics workstation, as a routine embedded in a dedicated electronic document, an electronic document viewer, or the like. The document and rights management system can also be implemented by physically incorporating the systems and methods into a hardware and/or software system, such as the hardware and software systems of a computer or dedicated electronic document.

[0062] It is, therefore, apparent that there has been provided, in accordance with the present invention, systems and methods for managing electronic documents. While this invention has been described in conjunction with a number of embodiments, it is evident that many alternatives, modifications and variations would be or are apparent to those of ordinary skill in the applicable art. Accordingly, applicants intend to embrace all such alternatives, modifications and variations that are within the spirit and scope of this invention.